



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,552	08/30/2001	Debbie Ann Godwin	AUS920010597US1	7626
45993	7590	03/07/2005	EXAMINER	
IBM CORPORATION (RHF) C/O ROBERT H. FRANTZ P. O. BOX 23324 OKLAHOMA CITY, OK 73123			ADAMS, JONATHAN R	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/942,552

Applicant(s)

GODWIN ET AL.

Examiner

Jonathan R Adams

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) _____ is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-15 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-15 rejected under 35 U.S.C. 103(a) as being unpatentable over Poletto et al., US PGP No 20020031134 (hereafter referred to as '134) in view of Terry Escamilla, "Intrusion Detection". "Computing the Moving Average of a Sequence" is provided as a defining reference for calculating moving averages.

3. As to claim(s) 1, 6, 11:

'134 teaches a method for detecting systematic attacks using system logs (Page 6, Paragraph 0073, '134) comprising:

- Establishing a float period length having a finite time duration / The gateways 26 and data collectors 28 keep statistical summary information of traffic over different periods of time (Page 6, Col 1, Line 1, '134)
- Counting a number of events in said event list which fall within said current float period / For example, a gateway 26 may keep mean and standard deviation for a

Art Unit: 2134

chosen set of parameters across a chosen set of time-periods (Page 6, Col 1, Lines 1-3, '134)

- Responsive to count exceeding a threshold, producing a violation message / The device will have configurable thresholds and will raise warnings when one of the measured parameters exceeds the corresponding threshold. (Page 6, Col 1, Lines 8-10, '134)
- Processing until float period end time exceeds a time stamp value of latest event in said event list / It is inherent that processing of a log file should cease at the end of the log file

4. '134 does not specifically teach the use of moving average statistical analysis.

Escamilla teaches the use of moving averages a beneficial statistical technique to detecting systematic attacks (Page 172, "Chief advantages of the statistical...", Escamilla), It would have been obvious to a person of ordinary skill in the art at the time of invention to use the moving average statistical approach to attack detection with the invention of '134. One of ordinary skill in the art would have been motivated to use the moving average statistical approach to attack detection with the invention of '134 because moving average is a "well-understood statistical technique" used to detect systematic attacks.

5. As to claim(s) 2, 7, 12:

Step of producing a violation message comprises creating a report viewable by a system administrator / The device will have configurable thresholds and will raise

Art Unit: 2134

warnings when one of the measured parameters exceeds the corresponding threshold.

(Page 6, Col 1, Lines 8-10, '134), This feature of the gateway enables administrators to quickly identify the important properties of the attack (Page 6, Paragraph 0073, '134)

6. As to claim(s) 3, 8, 13:

Producing a warning message if count is equal to or greater than one / The device will have configurable thresholds (Page 6, Col 1, Line 8, '134)

7. As to claim(s) 4, 9, 14:

Producing event list by accessing at least one host computer system audit file containing said events, extracting events from audit file and producing event list / Maintains a log of attack packets in a SAVE FILE (Page 22, "Description", '134)

8. As to claim(s) 5, 10, 15:

Counting only events for a single user / the parameters may include source (Page 6, Col 1, Line 4, '134)


Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is

Art Unit: 2134

(571)272-3832. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (571)272-3838. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100